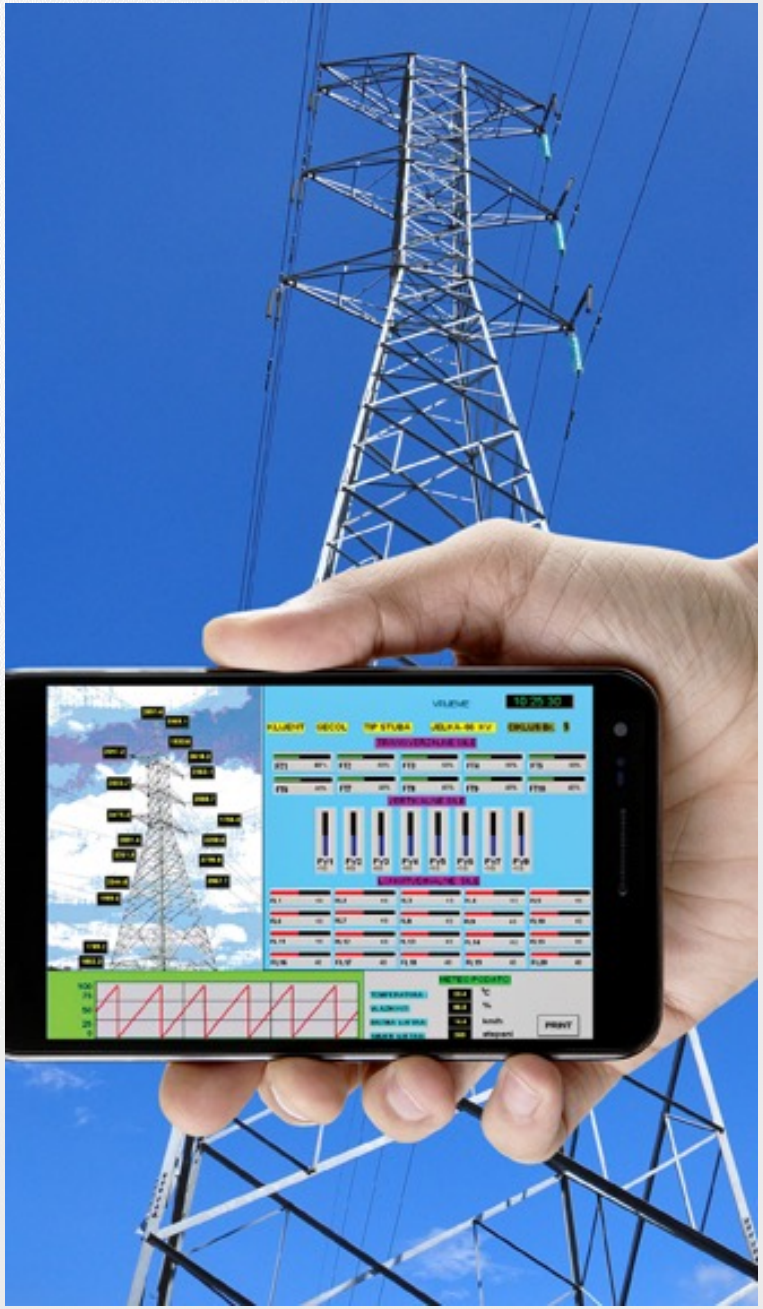
CYBER DEFENSE BY DESIGN

Industrial IoT e-Net
Registry/Information Clearinghouse &
Edge of Delivered Electron Intelligence
and Cyber Defense

Presented by:

Garland T. McCoy, President, Technology Education Institute
(gmccoy@technologyeducationinstitute.org)

Isiah Jones, Director of OT Security Solutions,
Fortress Information Services, LLC
(ijones@fortressinfosec.com)



• CONTENTS

- STANDARDS FIRST!
- RISK LEVELS RISING
- INDUSTRIAL IOT E-NET REGISTRY/INFORMATION CLEARINGHOUSE
- EDGE OF DELIVERED ELECTRON INTELLIGENCE & CYBER DEFENSE

ISA Setting the Standard for Automation

ISASecure®

Underwriters Laboratories Inc.®

NIST National Institute of Standards and Technology U.S. Department of Commerce

STANDARDS (DO NOT REINVENT THE WHEEL)!

- **Leverage security controls from existing standards**
  - Control selection, capabilities requirements
  - Contracts
  - Tailoring
  - Referencing multiple standards where one has gaps
- **Threat landscape is evolving but not that new**
  - Control systems with web services and RF/wireless communications have been around for years
  - Internet capable protocols have been deployed for years
  - Air gaps have eroded for years or did not truly exist at OSI layer 1, 2 and 7
- **Boots on the ground assessments tell the truth**
  - Independent neutral assessments, testing and validation teams
- **Community of Interest bully pulpit enforcement**
  - **DO NOT** wait for or rely on gov't regulation
  - **DO NOT** go it alone as a company in your sector
  - Look at interdependencies between sectors and leverage a community push for security controls

SUBSTATION ENERGY FLOW PIC

Reference:
https://www.osha.gov/SLTC/etools/electric_power/images/substation_energy_flow.jpg

Focus on Implementation and Execution

Referenced and Selected Standards	Capabilities & Requirements
• **ISA 62443 series** Broken into 7 FR areas with SR, CR, RE and SL 1 to 4 (Capability, Target, Achieved) • **NIST SP 800-53 rev4 and 82 rev 2** Broken into 18 Control families with a sub controls catalog and control enhancements and supplemental guidance for ICS/OT/Industrial IoT • **NIST SP 800 – 160** Lists and explains sound systems security engineering processes and steps to implement them • **Example Security Controls:** **FR-3 Systems Integrity (ISA 62443-3-3)** **SR 3.3 – Security functionality verification** **SL 1 to 4 –** required ability, including automated abilities, to demonstrate security features during FAT, SAT, Commissioning and Operations **SI – System Information and Integrity (NIST SP 800-53rev4 and 82 rev 2)** **SI-6 SECURITY FUNCTION VERIFICATION** **SI-6 (1), (2), (3)** – required reporting and automated capabilities to test and demo security features **NIS SP 800-160** **3.4.9 Verification Process** **VE-1, VE-2, VE-3 –** steps through preparation, performing and managing results of security feature verification of systems and components	**Contract Specs:** • List out must have minimum security controls and capabilities • **DO NOT** just say must comply with standard xyz • Make sure purchasing requirements include security capabilities within technical specs • Require control systems focused security training and certification from ISA, SCADAHacker and SANS ICS **Systems Integration:** • Site and system of system assessments prior to spending money on project construction and installs • Leverage frameworks and models not just the security controls in the standards • Build teams with IT and OT/ICS trained subject matter experts. Hire neutral third parties if necessary **Compliance is not Security:** • NERC CIP will not alone solve this issue – Transmission only – **DO NOT** need 50 state approaches or new standards • Improve by implementing security controls from existing cybersecurity and ICS/OT/Industrial IoT standards
Tailored Security Controls	**Assess, Validate, Test & Implement**
• Select security controls by site, systems, components and then roll them up to business unit and enterprise • **DO NOT** blindly select or implement all security controls and technical configurations	• Building site and system assessments into project plan and contract requirements • Build third party assessors, functional and acceptance testing and validation into project plan • Ensure continuous lifecycle of testing, verification and contract specification requirement updates

RTU WITH DOWN POWER LINE

Reference:
http://www.pumpsandsystems.com/sites/default/files/RTUWithDownPowerLine.jpg

WHERE DO WE GO FROM HERE?

- **Neutral** non-profit tracking, monitoring, assessment, training, development and advocacy organization supported by the community
  - Need asset owners and operators
  - Need academia
  - Need international, federal, state and local gov't
  - Need security researchers and security consultants
  - Need UL, ISA, NIST, IEC etc
  - Need OEMs at all stages of the supply chain
  - Need interns and professionals interested in a career change to ICS/OT security issues
- **DO NOT** just test, certify and move on
  - Need continuous monitoring
  - Make testing and certification and lifecycle
  - Improve certification documentation process (evolve the process to be continuous not just certifying a product version)
  - Track recertification of supply chain and system development process
  - Certify systems integration, testing, validation, acceptance and commission phases inclusion of safety and security controls and practices
- **Create templates:**
  - Verification checklist steps and tools that can be used as each step to help the asset owners and operators with low budget and low human resources
  - System security plans, test plans, contract technical specifications with specific security controls spelled out
  - Project plans that include security testing steps and roles, tools and skillsets needed for each task

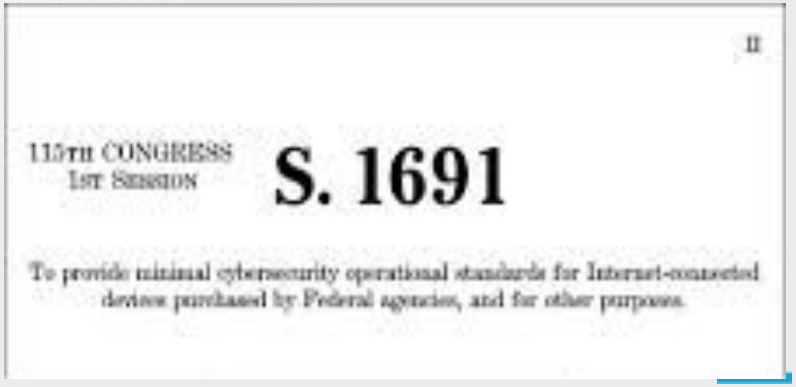
Reference: https://www.southcentralpower.com/wp-content/uploads/2016/07/2016_07_DS_TECH_TransformerWithRTU-684x1024.jpg

RISK LEVELS RISING – DRIVING POSTIVE & NEGATIVE OUTCOMES

- Pending litigation – led by the financial industry, where financial losses are clear, but *increasingly* critical infrastructure and reliability, customer safety, public and private property are at risk.
- IoT/IIoT devices (software/firmware) known to have significant security problems for decades despite standards – removing plausible deniability

- The critical importance of focusing on strategies to drive the regulatory and legislative focused momentum at the Federal level (transmission-Federal procurement) into State and Local Government agencies (procurement) and the grid's distribution network

- Insurance industry actively engaged in risk assessments in this area
- Potential for NERC CIP approach at Distribution level
  - 50 state approaches
  - Expanding CIP to state jurisdiction


II

115TH CONGRESS
1ST SESSION

S. 1691

To provide minimal cybersecurity operational standards for Internet-connected devices purchased by Federal agencies, and for other purposes.

E-NET REGISTRY & INFORMATION CLEARINGHOUSE

- **Registry listing**
  - Asset Owners and Operators (e.g. Utilities, Demand Contract customers)
  - OEMs
  - Integrators
  - Renewables & Storage (e.g DER, Smart Micro Grids, Solar, Wind, Geothermal)

- **Legacy IIoT devices**
  - Compliance in the stakeholders above
  - Devices would be upgraded, tracked and patched
  - Possible Tracking technologies (e.g. blockchain, DOA, dedicated block of IPV6 addresses with secure DNS, SDN)

- **Registry services catalogue**
  - Instillation, activation, lifecycle maintenance contracts
  - **ICS Guild**; Mentoring, tech training, listing of government-funded training centers, core curriculum recommendations and the creation of a pipeline for training graduates and hiring organizations in need of *human talent*

- **Registry Board and Council:**
  - Technical, academic and policy board members
  - Asset owners and operators, product makers, integrators, security researchers etc.

- **Registry Technical Data (not an exhaustive list)**
  - *What information would be available about the devices on the e-Net Registry?*
  - Collect aggregate information that OEMs register with UL and ISA secure testing and certification labs
  - General information about the assets such as commonly used ports, protocols, services, OS, hardware IC types etc
  - Who did the testing and where and when
  - Points of contact for lead technical SMEs within each OEM
  - From asset owners and operators: which integrators, EPCs, OEMs did the project installs, when, where etc
  - Contact information and survey information from asset owners and operators and/or independent security assessors as to how well security controls were implemented and what gaps remain with actionable mitigation recommendations

- **Private portal**
  - Open only to asset owners and operators, OEMs, and other registered members with a need to know of the information (e.g. ICS-CERT, registered independent assessors)

EDGE OF DELIVERED ELECTRON DEFENSE 1:
WHY IS IT NEEDED? WHAT HAS CHANGED? WHAT ARE THE RISKS?

- ***The edge of delivered electrons***
  - *The IoT/IIoT environment is where the cyber attack surface is the largest by many orders of magnitude on both sides of the meter and where it is the most porous*

- ***Customer/utility side of the meter***
  - *While cybercriminals have access to and are able to monitor and control infected IIoT devices through the customer's fiber optic, hybrid coax cable or G5 wireless networks at blazingly fast speeds, on the utilities side of the meter the communication network is slow and meter monitoring episodic*

- ***Generic devices***
  - *Substations at the distribution level have largely the same equipment manufactured by the same companies with the same cyber and physical security challenges as those managing transmission networks*

- ***Frontier mentality***
  - *The edge of delivered electrons is where most of the experimentation is ongoing in DC power generation and storage*

- ***Vast applicability***
  - *The edge of delivered electrons is where you will find; smart cities, electric car recharging stations, DERs and microgrids of every size*

- ***Real safety risks***
  - *Cyber attacks in the IIoT space have the demonstrated ability to pose significant risks to public safety and critical assets on both sides of the meter*

- ***The edge of delivered electrons in an IoT/IIoT enabled network is already an AC/DC Highway to Hell***

EDGE OF DELIVERED ELECTRON DEFENSE 2:
CHALLENGES AND POTENTIAL OPPORTUNITIES

CHALLENGES MANAGING THE IOT/IIOT ENABLED E-NET

- **Meter interface**
  - Generation and storage of DC power is growing exponentially
  - Utility lacks the ability to "see" or have any transparency on the customers side of the interconnection/meter
  - Human error and now the potential for cyber attacks impacting the DC to AC inverters/converters and power synchronization systems operation
  - Utilities approaching tolerance limits on having the ability to maintain operational control at the edge

Potential Opportunities

- **Smart Meters as intelligent sentries/listening posts at the edge of delivered electrons**
  - In the new IoT/IIoT enabled electron delivery network, the utility will not be able to manage load at the edge, or protect their assets and those of their customers under "normal operating conditions" as there will no longer be any expectation of "normal operating conditions" going forward
  - The "intelligence" we are building into the new e-Net, IIoT devices to be specific, are agnostic as to what "regulated" part of the "grid" they are operating in; transmission, distribution or customers side of the meter
  - When a cyber attack infects, captures and recruits IIoT devices embedded in electrical machines, devices, appliances into its botnet, it is also agnostic as to where these machine, appliances or devices reside along the network of delivered electrons
- **Leveraging underused assets**
  - Fiber, spectrum, power line communications, leased lines etc

EDGE OF DELIVERED ELECTRON DEFENSE 3:
WHAT MIGHT BE POSSIBLE?

- Is it possible to "deputize" smart meters, look at them as strategic assets, forward sentries or scouts, to build a "second line" of cyber defense based on the fact that there are two networks connected to electrical machines, devices and appliances?

- If smart meters represent an unused or underused asset in this space shouldn't we make an effort to experiment and see what is possible with the right communications, analytics and monitoring?

- If the electric utilities have unused and underused fiber assets should these assets not be considered for use in building an N2N encrypted VPN to backhaul intelligence gathered from the "forward sentries" (smart meters)?

- If it is the case that machines operate in "mechanical time" and the gap between mechanical time and modern communications and processing time is vast, then we should have ample time to detect and mitigate a significant amount of potential adverse effects of infected IIoT device launched cyber attacks on both sides of the smart meter.

- We have the off-the- shelf technology and tools to provide real-time intelligence and defense at the edge of delivered electrons that will protect lives and property on the entire e-network from generation to the end point of delivered electrons. Shouldn't we considering pressing these off the shelf technologies and unused or underused assets into service?

CONCLUSION

- In conclusion Isiah and I would like to stress the following; both of us have dedicated considerable amounts of our personal time to this book-of-work. I myself have been doing this on and off for several years now without pay

- This needs to be seen as a work-in- progress that both of us would like to suggest deserves your vetting/critique, continued engagement and support

- We need support to set up the 501c3 foundation that will anchor the e-Net Registry/Information Clearinghouse/Resource Center that will engage in the activities detailed in our presentation and will have a very distinguished group of leaders/stakeholders associated with its governance, management, and evolution.

- I want to close by acknowledging the support I have received from the following individuals who have helped, on their own personal time, to inform the body of this work.

ACKNOWLEDGEMENTS

- Vint Cerf, VP and Chief Internet Evangelist, Global Policy Development, Google *
- Isiah Jones, Director of OT Security Solutions, Fortress Information Security, LLC. *
- Bud Albright, Ogilvy Government Relations, former Under Secretary, DOE*
- Pat McCormick, Chief Counsel Senate Committee on Energy and Natural Resources *
- Nicholas Degani, Senior Counsel, FCC Chairman Ajit Pai*
- Galen Rasche, Senior Program Manager-Cyber Security, EPRI *
- Perry A. Pederson, ICS Cyber Security Program Manager, PNNL*
- Allan Friedman, Director Cybersecurity Initiatives, NTIA, Dept. of Commerce*
- Tony Alexander, Former CEO FirstEnergy*
- Ken Modeste, Chief of Cybersecurity & Technology Services, UL-CAP*
- Andre Ristaino, Managing Director, Automation Standards Compliance Institute (ISASecure) *
- Daniel Phillips, Director, Cyber Risk Engineering, Axio*
- Daryl Haegley, Program Manager, Information Risk Manager, Business Enterprise Integration Directorate, Office of the Deputy Under Secretary of Defense, DOD. *
- Ray Palmer, Chief, Energy Innovations Sector, FERC*
- Robert Ivanauskas, Public Advisor, FERC*
- Nita Crowley, Partner, WilmerHale (retired) *
- David Owens, Former Executive VP Business Operations and Regulatory Affairs, EEI
- Lee W. McKnight, Associate Professor, School of Information Studies, Syracuse University
- Douglas Sicker, Thomas Lord Endowed Chair, Department Head of Engineering and Public Policy, Professor of Engineering and Computer Science, Carnegie Mellon University, AD0VT
- Jody Westby, CEO, Global Cyber Risk, LLC
- Thomas Lind, School of International and Public Affairs, Columbia University

I want to emphasize that individuals listed participated on their own time and their involvement does not convey any official endorsement from their employer.

* July 10th Dinner Attendees